AMENDMENTS TO SPECIFICATION

♦ **Headers**

Please insert the following headers into the specification at the indicated locations:

Page 1, before line 1 (but after the title):

–BACKGROUND OF THE INVENTION

1. Field of the Invention–.

Page 1, between lines 2 and 3:

–2. Description of Related Art–.

Page 1, before line 25, but after the insertion made in the preliminary amendment submitted February 14, 2001:

–SUMMARY OF THE INVENTION–.

Page 4, between lines 18 and 19:

–BRIEF DESCRIPTION OF THE DRAWINGS–.

Page 4, between lines 28 and 29:

–DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS–.

♦ **Other Changes to the Specification**

Please amend the following paragraphs of the specification:

Page 1, line 27:

This problem is solved by ~~the feature combinations of the independent claims~~ limiting the semiconductor chip of a data carrier to executing operating program commands of a such a kind, or executing the commands in such a way, that the data processed with the corresponding commands cannot be inferred from signals detectable from outside the semiconductor chip.

Page 3, lines 3-19:

In order to guarantee the functioning of the data carrier one must ensure that the data carrier delivers the right results when rightfully used despite the falsified secret data. This is obtained by first specifying a function for falsifying the authentic secret data, for example ~~EXORing~~ XORing the secret data with a random number. The authentic secret data are falsified with the thus specified function. The falsified secret data are used to perform all those operations in the data carrier ~~in~~ for which falsification of the secret data can subsequently be compensated. In the case of ~~EXOR-falsified~~ XOR-falsified secret data, these would be operations which are linear with respect to ~~EXOR~~ XOR operations. Before execution of an operation not permitting such compensation, for example an operation which is nonlinear with respect to ~~EXOR~~ XOR operations, the authentic secret data must be restored so that said operation is performed with the authentic secret data. The authentic secret data are restored after execution of a compensable function for example by ~~EXORing~~ XORing the function value determined by means of the falsified secret data with a corresponding function value of the random number used for falsification. It is important in this context for the random number and function value to be previously determined and stored in safe surroundings so that the calculation of the function value from the random number cannot be intercepted.

Page 6, line 22 to Page 7, line 13:

Fig. 3 shows a schematic representation of part of an operational sequence in the smart card. An encryption operation was selected for the representation by way of example. However, the principles explained by this example are also applicable to any other security-relevant operations. At the onset of the part of the encryption operation shown in Fig. 3, data *abc*, which can be present in plaintext or already encrypted, are supplied to logic point 7. At logic point 7 data *abc* are combined with key $K1$. In the present example this combination is an ~~EXOR~~ XOR operation but other suitable forms of combination can also be used. Nonlinear function g is then applied to the result of the combination in function block 8. In order to show that function block 8 represents a nonlinear function it has the form of a distorted rectangle in Fig. 3. The data produced with function block 8 are ~~EXORed~~ XORed with random number Z at logic point 9 and

subsequently processed in function block 10. Combination with random number Z causes falsification of the data which makes it difficult for an attacker to analyze the processes in function block 10 representing a linear mapping by means of function f. an undistorted rectangle is used as a symbol of a linear function in Fig. 3. The data produced in function block 10 are combined at logic point 11 with data $f(Z)$ previously generated e.g. during production of the card by application of function f to random number Z. This combination compensates for the falsification of the data with random number Z at logic point 9. Said compensation is necessary since nonlinear function g is subsequently to be applied to the data in function block 12 and compensation of falsification is no longer possible after application of a nonlinear function to the data. Further, the data are ~~EXORed~~ XORed at logic point 11 with key $K2$ which is necessary in connection with the encryption operation.

Page 7, lines 14-20:

The combination at logic point 11 with the data $f(Z)$ and $K2$ can be effected either with single components $K2$ and $f(Z)$ or with the result of an ~~EXOR~~ XOR operation of said components. The latter procedure opens up the possibility of key $K2$ not needing to be available in plaintext but only key $K2$ ~~EXORed~~ XORed with $f(Z)$. If this combination value was calculated and stored in the memory of the card previously, e.g. during initialization or personalization of smart card 1, it is unnecessary to store key $K2$ in smart card 1 in plaintext. This further increases the security of smart card 1.

Page 7, lines 21-26:

After application of function g to the data in function block 12 the thus determined result is in turn combined with random number Z at logic point 13 and thereby falsified. Linear function f is then applied to the result of the combination in function block 14. Finally, the data are ~~EXORed~~ XORed with the result of an application of function f to random number Z and with key $K3$ at logic point 15. This operation can be followed by further processing steps not shown in Fig. 3.

Page 7, line 27 to Page 8, line 7:

All in all, the procedure shown in Fig. 3 can be summarized by saying that the data processed in the encryption operation are falsified whenever possible by ~~EXORing~~ XORing with random number Z in order to prevent secret data from being spied out. Falsification is fundamentally possible with all functions f showing linear behavior with respect to ~~EXOR~~ XOR operations. With nonlinear functions g the unfalsified data must be used. It is therefore necessary that the falsification be compensated by ~~EXORing~~ XORing the data with function value $f(Z)$ before application of nonlinear function g to the data. It is less critical from a security point of view that nonlinear functions g can only be applied to the unfalsified data since said nonlinear functions g are much more difficult to spy out than linear functions f. the diagram shown in Fig. 3 is applicable both for identical functions g or functions f and for different respective functions.